

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF THE CLAIMS:

1. (Currently Amended) A method of providing anonymous digital cash, said method comprising:
 - providing an entity with a secure co-processor;
 - a user establishing a secure channel to a program running on said coprocessor;
 - the user sending a coin to be digitally signed to the coprocessor using any secure digital signature algorithm; and
 - signing the coin with a non-homomorphic signature and sending back to the user both an encrypted copy of the signed coin and an encrypted copy of the unsigned coin to enable the user to use the coin while keeping the identity of the user unknown to the coprocessor.
2. (Original) A method according to Claim 1, further comprising the steps of:
 - the processor providing a signature to authenticate;
 - the user using said coin for payment to a merchant; and
 - the merchant returning the signed coin to the entity for credit to an account of the merchant.
3. (Currently Amended) A method of creating and managing electronic cash, comprising the steps:
 - a customer communicating to a secure cryptography generator an encryption scheme and a cash amount;
 - establishing a unit representing the cash amount;

BEST AVAILABLE COPY

signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the coprocessor;
using the secure cryptography generator to encrypt the signed unit and to encrypt the unsigned unit using the encryption scheme;
storing in a database the encrypted signed unit and a value for the unit;
transmitting the encrypted signed unit back to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit;
the customer decrypting the encrypted signed unit to obtain the signed unit; and
using the signed unit as a payment.

4. (Original) A method according to Claim 3, further including the steps of:
establishing an expiration date for the unit; and
storing the expiration date in the database.
5. (Original) A method according to Claim 3, wherein the signing step includes the step of using the secure cryptography generator to sign the unit.
6. (Cancelled).
7. (Currently Amended) A system for creating and managing electronic cash, comprising the steps:
a secure cryptography generator, including means for receiving an encryption scheme and a cash amount from a customer;
means for establishing a unit representing the cash amount;

means for signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the coprocessor;

wherein the secure cryptography generator encrypt the signed unit and encrypts the unsigned unit using the encryption scheme;

a database for storing the encrypted signed unit and a value for the unit;

means for transmitting ~~the encrypted signed unit back~~ to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit; and

means for the customer to decrypt the encrypted signed unit to obtain the signed unit, wherein the customer is able to use the signed unit as a payment.

8. (Original) A system according to Claim 7, further including means for establishing an expiration date for the unit, and wherein the expiration date is stored in the database.

9. (Original) A system according to Claim 7, wherein the secure cryptography generator includes means for signing the unit.

10. (Cancelled).

11. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for creating and managing electronic cash, said method steps comprising:

using a secure cryptography generator to receive from a customer an encryption scheme and a cash amount;

establishing a unit representing the cash amount;

signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the coprocessor;[[;]]

using the secure cryptography generator to encrypt the signed unit and to encrypt the unsigned unit using the encryption scheme;

storing in a database the encrypted signed unit and a value for the unit;

transmitting ~~the encrypted signed unit back~~ to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit;

decrypting the encrypted signed unit to obtain the signed unit; and

using the signed unit as a payment.

12. (Original) A program storage device according to Claim 11, wherein said method steps further include the steps of:

establishing an expiration date for the unit; and

storing the expiration date in the database.

13. (Original) A program storage device according to Claim 11, wherein the signing step includes the step of using the secure cryptography generator to sign the unit.

14. (Cancelled).

15. (Previously Presented) A method according to Claim 2, wherein:
the encryption scheme has a public key and a private key;

the communicating step includes the step of the customer sending to the generator the public key of the encryption scheme; and

the step of using the secure cryptography generator includes the step of using the public key to encrypt the signature on the unit.

16. (Previously Presented) A method according to Claim 15, wherein:

the signing step includes the step of using a non-homomorphic signature scheme to sign the unit;

the non-homomorphic signature scheme includes a private key and a public key; and

the step of using the non-homomorphic signature scheme includes the step of using the private key of the non-homomorphic signature scheme to sign the unit.